1. The value proposition for participating as a CIKR partner within the NIPP framework refers to:

   a. The funding provided by the Federal Government to local jurisdictions for the development and implementation of protection programs
   b. The expertise within the Government for protecting the country's infrastructure against terrorist attacks
   c. The research and development initiatives being conducted by the academic community to enhance infrastructure protection technology
   d. The benefits gained from the public private partnership

2. The scope of the NIPP is designed to address which of the following types of events?

   a. A virus that attacks multiple companies' computer systems
   b. A localized flood that causes dirt roads in a rural county to wash out
   c. A military attack overseas on U.S. interests
   d. A mass murder in London

3. Which of the following statements about the NIPP is FALSE?

   a. The NIPP framework is applicable for both terrorist attacks and natural disasters
   b. The NIPP replaces a business' continuity of operations and emergency operations plans
   c. The NIPP approach is to foster collaboration between the private sector and the public sector
   d. The NIPP's risk management framework allows for differences based on unique sector characteristics

4. Which of the following is NOT an example of critical infrastructure covered by the NIPP?

   a. Nuclear power plants
   b. Agricultural distribution centers
   c. Military installation
   d. Highways and bridges

5. The NIPP advocates that the Government and private sector partners participate in multidirectional exchange of information. The NIPP refers to this as:

   a. Hierarchal information sharing
   b. Cyber information sharing
   c. Networked information sharing
   d. Open-source information sharing

6. What provides the basis for Department of Homeland Security (DHS) responsibilities in the protection of the Nation's CIKR?

   a. The Homeland Security Presidential Directive 5 (HSPD-5)
   b. The National Incident Management System (NIMS)
   c. The National Response Framework (NRF)
   d. The Homeland Security Act of 2002

7. Sector-Specific Agencies (SSAs) are responsible for:

   a. Developing Sector-Specific Plans to guide the CIKR protection and resiliency efforts throughout their sector
   b. Funding the implementation of optimal protection programs proposed by State, local, and tribal entities
   c. Evaluating the effectiveness of mandatory protection measures implemented by the private sector and industry
   d. Providing advice to the Secretary of Homeland Security on cross-sector security issues related to critical infrastructure

8. What is the name of the group (composed of private industry, academia, and State and local government representatives) that provides the President with advice on the security of the critical infrastructure sectors and their information systems?

   a. Homeland Security Council (HSC)
   b. National Infrastructure Advisory Council (NIAC)
   c. Federal Leadership Advisory Council (FLAC)
   d. Critical Infrastructure Protection Advisory Council (CIPAC)

9. Which of the following CIKR partners are most likely to establish Centers of Excellence to provide independent analysis of CIKR protection issues?

   a. The academic community
   b. Federal agencies
   c. NIPP councils
   d. State, local, and tribal governments

10. The Critical Infrastructure Partnership Advisory Council (CIPAC) facilitates effective coordination between Federal CIKR partners and:

    a. Agencies and organizations within the Department of Homeland Security
    b. Private sector and State, local, territorial, and tribal governments
    c. Federal agencies and departments that are designated as sector-specific agencies
    d. Nongovernmental organizations within designated high-risk regions

11. Sector-specific NIPP planning and coordination are addressed through the:

    a. Sector Coordinating Councils (SCC)
    b. Infrastructure Policy Coordinating Committee (I-PCC)
    c. Homeland Security Information Network for Critical Sectors (HSIN-CS)
    d. Federal Sector Leadership Council (FSLC)

12. In the context of the NIPP, risk is defined as:

    a. The elements within an asset, system, or network's design, location, or operation that render it susceptible to destruction
    b. The estimated magnitude of financial loss or damage that can be expected from a terrorist attack or natural disaster
    c. The likelihood that a particular asset, system, or network will suffer a terrorist attack or a natural disaster
    d. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

13. Read the following definition and select the correct component of risk: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

    a. Consequences
    b. Vulnerability
    c. Threat

14. One step in the NIPP risk management framework is to:

    a. Identify assets, system and networks
    b. Define roles and responsibilities
    c. Estimate budgetary needs
    d. Determine implementation timeframes

15. The risk management framework is comprehensive and takes into account CIKR assets, systems, and networks. It also considers the following elements:

    - Physical
    - Cyber
    - _____

    a. Resiliency
    b. Financial
    c. Human
    d. Policies

16. Risk assessment results can inform all of the following decisions, EXCEPT FOR:

    a. DHS grant allocations
    b. Allocation of response and recovery resources during an incident
    c. Evaluating regulatory compliance with the Federal infrastructure protection policies and procedures
    d. Identifying gaps and requirements for protective measures and actions

17. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of:

    a. A single point of failure
    b. A loss of competitive edge in the international marketplace
    c. A negative effect on the Nation's economy and the public health and safety of the citizens
    d. An attack being attempted by an adversary

18. Protective actions or programs are designed to manage risks by:

    - Deterring threats
    - Minimizing consequences
    - _____

    a. Eliminating consequences
    b. Mitigating vulnerabilities
    c. Counteracting consequences
    d. Neutralizing consequences

19. According to the NIPP, a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property is the:

    a. Risk
    b. Consequence
    c. Vulnerability
    d. Threat

20. Sector-Specific Plans are:

    a. Developed by the Sector-Specific Agencies and tailored to address the unique characteristics of each sector
    b. Submitted by State, local, and tribal governments who receive Homeland Security grants
    c. Required as part of the Federal Government regulatory oversight of vulnerable industries
    d. Designed to provide specific guidance for incorporation into local emergency operations plans

21. The NIPP and the National Response Framework (NRF) work together to provide a comprehensive, integrated approach to the homeland security mission. The NRF provides:

    a. The detailed risk management model for CIKR protection
    b. The approach for domestic incident management
    c. The system used to allocate resources for CIKR protection
    d. The measures of CIKR protection program effectiveness

22. To ensure an effective, efficient CIKR protection program over the long term, the NIPP relies on all of the following EXCEPT FOR:

    a. Enabling education, training, and exercise programs
    b. Creating mandatory programs regulated by DHS
    c. Conducting R&D and using technology
    d. Developing, protecting, and maintaining data systems and simulations

23. Which program includes procedures that govern the receipt, validation, handling, dissemination, storage, marking, and use of critical infrastructure information voluntarily submitted to the Department of Homeland Security?

    a. Protective Security Advisor Program
    b. Control Systems Security Initiative
    c. Protected Critical Infrastructure Information (PCII) Program
    d. Protective Community Support Program

24. The NIPP:

    a. Recognizes that the disclosure of sensitive business or security information could cause serious damage to companies, the economy, public safety, or security
    b. Mandates that State and local government disclose sensitive security information to all CIKR partners within their jurisdictions
    c. Establishes reporting formats for the disclosure of sensitive CIKR security information by government agencies to the public
    d. Prohibits the government from requesting sensitive business information from private sector partners

25. According to the NIPP, effective protective actions and programs are:

    - Comprehensive.
    - Coordinated.
    - Cost effective.
    - _____

    a. DHS approved
    b Regionally centered
    c. Industry certified
    d. Risk-informed